Journal of Number Theory 77, 252–273 (1999)
Article ID jnth.1999.2385, available online at http://www.idealibrary.com on IDEAL®

Integral Galois Module Structure of Some Lubin–Tate Extensions

Nigel P. Byott

School of Mathematical Sciences, University of Exeter, Exeter EX4 4QE, United Kingdom
E-mail: N.P.Byott@ex.ac.uk

Communicated by A. C. Woods

Received July 7, 1998

Let K be a finite extension of $\mathbb{Q}_p$, and suppose that $K/\mathbb{Q}_p$ is ramified and that the

$\mathfrak{O}^{(2)}$ is not free over this order. The integral Galois module structure of certain intermediate fields E of $K^{(2)}/K$ is also considered. In particular, if $p \neq 2$ and K has residue field of cardinality p or p^2, we show that the valuation ring of E is free over its associated order if and only if E/K is either tamely ramified or a p-extension. We also prove that the valuation ring of any weakly ramified abelian extension of K is free over its associated order. © 1999 Academic Press

INTRODUCTION

Let K be a finite extension of the p-adic field $\mathbb{Q}_p$, and let $\mathfrak{o} = \mathfrak{O}_K$ denote its valuation ring. Let L be a finite normal extension of K, with Galois group $\Gamma = \mathrm{Gal}(L/K)$. We will be concerned with the structure of the valuation ring $\mathfrak{O}_L$ of L as a module over its associated order

$$\mathfrak{A}_{L/K} = \{\alpha \in K\Gamma \mid \alpha \cdot \mathfrak{O}_L \subseteq \mathfrak{O}_L\}$$

in the group algebra $K\Gamma$. It is well-known that $\mathfrak{A}_{L/K}$ coincides with the integral group ring $\mathfrak{o}\Gamma$ precisely when L/K is at most tamely ramified, and that in this case $\mathfrak{O}_L$ is a free $\mathfrak{o}\Gamma$-module.

If $K = \mathbb{Q}_p$ and L is abelian over $\mathbb{Q}_p$, then $\mathfrak{O}_L$ is a free $\mathfrak{A}_{L/\mathbb{Q}_p}$-module. This is the local version of an old result of H.-W. Leopoldt [13] on absolutely abelian number fields. Recently, G. Lettl [14] has shown that if L is abelian over $\mathbb{Q}_p$, but now K is any intermediate field of the extension $L/\mathbb{Q}_p$, then again $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$. This property in fact characterises $\mathbb{Q}_p$ among its finite extensions: the nth division field $K^{(n)}$ of K with respect

0022-314X/99 $30.00

to a Lubin–Tate formal group is an abelian extension of K, but by [3, Theorem 5.1], $\mathfrak{O}_{K^{(m+r)}}$ fails to be free over $\mathfrak{A}_{K^{(m+r)}/K^{(r)}}$ whenever $m > r$ and $K \neq \mathbb{Q}_p$. It is therefore of some interest to determine, for a given $K \neq \mathbb{Q}_p$, which fields L in some suitable class of abelian extensions of K have the property that $\mathfrak{O}_L$ is, or is not, free over $\mathfrak{A}_{L/K}$. One knows from the treatment of local class field theory via Lubin–Tate extensions (see for instance [17]) that every finite abelian extension of K is contained in the compositum of some division field $K^{(n)}$ and some unramified extension. Thus a natural (though rather too large) class of extensions to consider is the class of subfields L of the fields $K^{(n)}$. An understanding of $\mathfrak{O}_L$ for all such L would take us a long way towards determining the integral Galois module structure of all finite abelian extensions of K.

In this paper, we give some partial results in this direction. We consider only the extension $K^{(2)}/K$ and certain of its intermediate fields, often under the hypotheses that K is ramified over $\mathbb{Q}_p$ and that $p \neq 2$. Our treatment of the intermediate fields uses a result, whose proof we give elsewhere [5], on sums over a finite additive subgroup of a field. We are able to handle *all* intermediate fields of the extension $K^{(2)}/K$ only in the case that $\mathfrak{o}$ has residue field of cardinality p or p^2. As a consequence of our results, we show that if L is any weakly ramified abelian extension of K then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$.

Although the integral Galois module structure of extensions of the form $K^{(m+r)}/K^{(r)}$ has been considered in some detail (see [3, 4, 7, 8, 18, 19]), I am not aware of any previous investigation of the extensions $K^{(n)}/K$, with K itself as base field.

Our explicit results on the valuation ring of $K^{(2)}$ and its associated order (Theorem 1, Lemmas 2.12 and 2.20, and Corollary 2.28) bear a striking similarity to recent work of R. Miller [15], who considers the corresponding problem for function fields in characteristic p. In that setting, the Lubin–Tate formal group is replaced by the Carlitz module.

I thank David Burns, Robin Chapman, and Günter Lettl for helpful conversations about this work.

1. NOTATION AND STATEMENT OF RESULTS

Throughout, K is a finite extension of $\mathbb{Q}_p$, with further hypotheses imposed from time to time. We write $\mathfrak{o}$ for the valuation ring $\mathfrak{O}_K$ of K. Let q be the cardinality of the residue field of $\mathfrak{o}$, and let π be a uniformising parameter of $\mathfrak{o}$. Except in Section 4, we take π to be fixed and therefore do not indicate dependence on π in our notation.

Let $f(X)$ be a Lubin–Tate series for K, corresponding to the parameter π, and let $F(X, Y)$ be the formal group admitting $f(X)$ as an

endomorphism. (For background on Lubin–Tate theory, see [17].) Let $\mathfrak{m}$ be the maximal ideal of the valuation ring of a fixed algebraic closure of K, and set

$$G^{(n)} = \{\omega \in \mathfrak{m} \mid f^{(n)}(\omega) = 0\}, \qquad n \geqslant 0,$$

where $f^{(0)}(X) = X$ and $f^{(n)}(X) = f(f^{(n-1)}(X))$ for $n \geqslant 1$. Then the division fields $K^{(n)}$ are defined by $K^{(n)} = K(G^{(n)})$.

For each $\alpha \in \mathfrak{o}$ there is a unique endomorphism $[\alpha](X)$ of $F(X, Y)$ with linear term αX. If α lies in the group of units $\mathfrak{o}^\times$ of $\mathfrak{o}$ then $[\alpha](X)$ determines an automorphism $\langle \alpha \rangle$ of the field $K^{(n)}$ with $\langle \alpha \rangle(\omega) = [\alpha](\omega)$ for all $\omega \in G^{(n)}$. This induces an isomorphism of groups between $(\mathfrak{o}/\pi^n\mathfrak{o})^\times$ and $\Gamma^{(n)} = \mathrm{Gal}(K^{(n)}/K)$.

We now set $\tilde{\Gamma} = \Gamma^{(2)} = \mathrm{Gal}(K^{(2)}/K)$. Abusing notation, we identify the quotient $\Gamma^{(1)} = \mathrm{Gal}(K^{(1)}/K)$ of $\tilde{\Gamma}$ with the subgroup of $\tilde{\Gamma}$ consisting of elements of order prime to p. Thus

$$\tilde{\Gamma} = \Gamma^{(1)} \times \Gamma$$

where

$$\Gamma = \{\langle 1 + \pi\alpha \rangle \mid \alpha \in \mathfrak{o}\}$$

and

$$\Gamma^{(1)} = \{\langle \mu \rangle \mid \mu^{q-1} = 1\}.$$

Here $\Gamma^{(1)}$ is cyclic of order $q-1$, and Γ is elementary abelian of order q, being isomorphic to the additive group $\mathfrak{o}/\pi\mathfrak{o}$ via $\langle 1 + \pi\alpha \rangle \mapsto (\alpha \bmod \pi\mathfrak{o})$. Let K' be the fixed field of $K^{(2)}$ under $\Gamma^{(1)}$. We identify $\Gamma = \mathrm{Gal}(K^{(2)}/K^{(1)})$ with $\mathrm{Gal}(K'/K)$ by restriction.

The fields introduced so far, together with the various Galois groups and extension degrees, are as indicated in Fig. 1. If we think of the fields K, K', $K^{(1)}$, $K^{(2)}$ schematically as lying at the vertices of a parallelogram, then the other intermediate fields of the extension $K^{(2)}/K$ correspond to points either on the edges of the parallelogram or in its interior. We shall consider certain of these intermediate fields, as shown in Fig. 2.

We abbreviate $\mathfrak{O}_{K^{(1)}}$, $\mathfrak{O}_{K^{(2)}}$, and $\mathfrak{O}_{K'}$ to $\mathfrak{O}^{(1)}$, $\mathfrak{O}^{(2)}$, and $\mathfrak{O}'$, respectively.

For any finite group Δ, let T_Δ denote the trace element of the group ring $\mathfrak{o}\Delta$,

$$T_\Delta = \sum_{\delta \in \Delta} \delta.$$

Also, let $(\mathfrak{o}\Delta)^+$ denote the augmentation ideal of $\mathfrak{o}\Delta$. Thus $(\mathfrak{o}\Delta)^+$ is a free $\mathfrak{o}$-module on the basis $\{\delta - 1 \mid \delta \in \Delta \backslash \{1\}\}$.

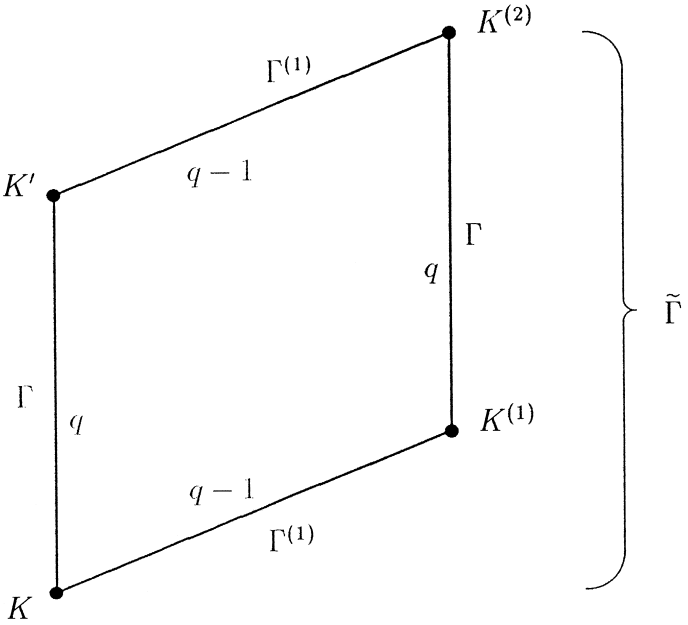

FIG. 1. Extension degrees and Galois groups.

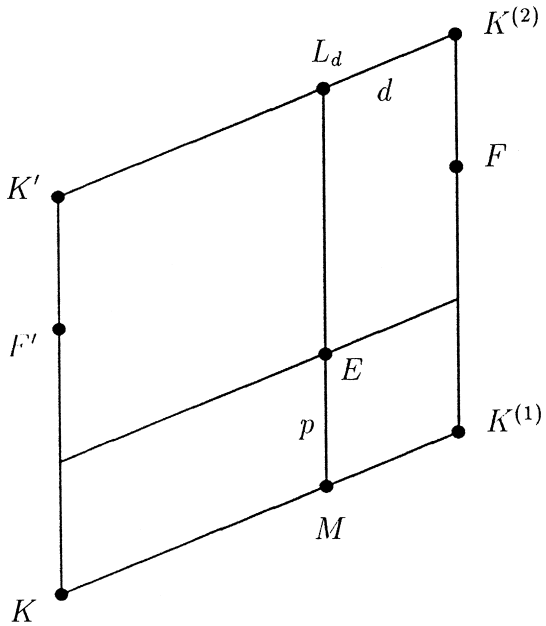

FIG. 2. Intermediate fields considered.

Our first result concerns the fields along the upper edge of the parallelogram of Fig. 2. For any divisor d of $q-1$, let L_d be the unique intermediate field of $K^{(2)}/K$ with $[K^{(2)}: L_d] = d$. Thus $L_d \supseteq K'$, and in particular $L_{q-1} = K'$ and $L_1 = K^{(2)}$. For any finite extension L of $\mathbb{Q}_p$, we write $v_L: L \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ for the normalised valuation on L.

THEOREM 1. (i) *The associated order* $\mathfrak{A}_{K'/K}$ *is* $\mathfrak{o}\Gamma[\pi^{-1}T_\Gamma]$, *and* $\mathfrak{O}'$ *is free as a module over* $\mathfrak{A}_{K'/K}$. *In fact,* $\mathfrak{O}' = \mathfrak{A}_{K'/K} \cdot \beta$ *for any* $\beta \in \mathfrak{O}'$ *with* $v_{K'}(\beta) = 1$.

(ii) *Suppose that* K *is ramified over* $\mathbb{Q}_p$, *and let* $d \neq q-1$ *be a divisor of* $q-1$. *Then* $\mathfrak{O}_{L_d}$ *is not free over* $\mathfrak{A}_{L_d/K}$. *In particular, if* $q \neq 2$ *then* $\mathfrak{O}^{(2)}$ *is not free* $\mathfrak{A}_{K^{(2)}/K}$.

The associated orders occurring in Theorem 1(ii) are described explicitly in Corollary 2.28.

The fields M along the lower edge of the parallelogram are tamely ramified over K. Thus $\mathfrak{A}_{M/K}$ is just the integral group ring, and $\mathfrak{O}_M$ is free over $\mathfrak{A}_{M/K}$. Our next two results deal with fields on the vertical edges of the parallelogram.

THEOREM 2. *Let* F' *be an intermediate field of the extension* K'/K, *and let* $\Delta = \mathrm{Gal}(F'/K)$. *Thus* $\mathfrak{A}_{F'/K} = \mathfrak{o}\Delta[\pi^{-1}T_\Delta]$, *and* $\mathfrak{O}_{F'}$ *is free over* $\mathfrak{A}_{F'/K}$. *In fact,* $\mathfrak{O}_{F'} = \mathfrak{A}_{F'/K} \cdot \beta$ *for any* $\beta \in \mathfrak{O}_{F'}$ *with* $v_{F'}(\beta) = 1$.

THEOREM 3. *Suppose that* K *is ramified over* $\mathbb{Q}_p$. *Let* F *be an intermediate field of the extension* $K^{(2)}/K^{(1)}$ *with* $[F: K^{(1)}] > 2$. *Then* $\mathfrak{O}_F$ *is not free over* $\mathfrak{A}_{F/K}$.

We have now considered all fields on the edges of the parallelogram of Fig. 2, at least when $K/\mathbb{Q}_p$ is ramified and $p \neq 2$. In general, there are further intermediate fields of $K^{(2)}/K$, corresponding to interior points of the parallelogram. Our methods do not enable us to handle all of these, but we can deal with the "bottom layer" of interior fields, namely those fields E for which $[E:K]$ is divisible by p but not by p^2.

THEOREM 4. *Suppose that* K *is ramified over* $\mathbb{Q}_p$, *that* $p \neq 2$, *and that* $q \geqslant p^2$. *Let* E *be an intermediate field of the extension* $K^{(2)}/K$ *such that* $E \not\subseteq K'$, $E \not\subseteq K^{(1)}$, *and* $[E:K]$ *is not divisible by* p^2. *Then* $\mathfrak{O}_E$ *is not free* $\mathfrak{A}_{E/K}$.

The case $p = 2$ is a genuine exception: $\mathfrak{O}_E$ is free over $\mathfrak{A}_{E/K}$ for all E satisfying the conditions stated (see after Lemma 5.6).

We will in fact prove a slightly stronger result than Theorem 4 (see Theorem 6 at the end of the paper), and, again, we will give an explicit description of the associated orders occurring.

If $q = p$ there are no fields in the interior of the parallelogram of Fig. 2, and if $q = p^2$ then all the interior fields are covered by Theorem 4 unless $p = 2$. We can therefore summarise Theorems 2, 3 and 4 in these two cases as follows:

COROLLARY 1.1. *Suppose that K is ramified over $\mathbb{Q}_p$ and that either $q = p$ or $q = p^2 \neq 4$. Let E be any intermediate field of $K^{(2)}/K$. Then $\mathfrak{O}_E$ is free over $\mathfrak{A}_{E/K}$ if and only if E/K is either tamely ramified (so $E \subseteq K^{(1)}$) or of p-power degree (so $E \subseteq K'$).*

It would be interesting to know whether the conclusion of Corollary 1.1 holds for arbitrary odd q.

Finally, we record a result which does not specifically concern Lubin–Tate extensions, but which is a consequence of Theorem 2. Recall that if F is any finite normal extension of K, with $\mathrm{Gal}(F/K) = \Delta$, say, then the ramification groups of F/K (in the lower numbering) are the groups

$$\Delta_i = \{\delta \in \Delta \mid (\delta - 1)\,\mathfrak{O}_F \subseteq \mathfrak{P}_F^{i+1}\}$$

where $\mathfrak{P}_F$ is the maximal ideal of $\mathfrak{O}_F$. Thus Δ_0 is the inertia subgroup of Δ, and Δ_1 is the "wild" ramification group. The extension F/K is said to be weakly ramified if Δ_2 is trivial. Various Galois module results involving such extensions can be found in [1, 9–11, and 20]. In particular, S. Ullom [20] has shown that if F/K is totally and weakly ramified (but not necessarily abelian) then $\mathfrak{P}_F$ is free over $\mathfrak{o}\Delta$. It follows easily from this that $\mathfrak{O}_F$ is free over $\mathfrak{o}\Delta[\pi^{-1}T_\Delta]$. In Section 4, we relate weakly ramified abelian extensions to Lubin–Tate theory, thereby obtaining the following result:

THEOREM 5. *Let F be any weakly ramified abelian extension of K (not necessarily totally ramified). Let $\Delta = \mathrm{Gal}(F/K)$. Then $\mathfrak{A}_{F/K} = \mathfrak{o}\Delta[\pi^{-1}T_{\Delta_0}]$, and $\mathfrak{O}_F$ is free over $\mathfrak{A}_{F/K}$.*

2. DESCRIPTION OF $\mathfrak{A}_{K^{(2)}/K}$

In this Section, which forms the heart of the paper, we obtain an explicit description of the associated order $\mathfrak{A}_{K^{(2)}/K}$ and use it to prove Theorem 1.

The group ring $\mathfrak{o}\Gamma^{(1)}$ has an $\mathfrak{o}$-basis of idempotents

$$\varepsilon_i = \frac{1}{q-1} \sum_{\mu^{q-1}=1} \mu^{-1}\langle \mu \rangle, \qquad 0 \leqslant i \leqslant q-2. \tag{2.1}$$

For each i, we have $K\tilde{\Gamma}\varepsilon_i \cong K\Gamma$ as K-algebras. The inverse isomorphism is given by $\gamma \mapsto \gamma\varepsilon_i$ for $\gamma \in K\Gamma$. Thus

$$\mathfrak{o}\tilde{\Gamma} = \prod_{i=0}^{q-2} \mathfrak{o}\tilde{\Gamma}\varepsilon_i = \prod_{i=0}^{q-2} \mathfrak{o}\Gamma\varepsilon_i$$

and we have decompositions

$$\mathfrak{D}^{(2)} = \bigoplus_{i=0}^{q-2} \varepsilon_i \mathfrak{D}^{(2)}, \qquad \mathfrak{A}_{K^{(2)}/K} = \prod_{i=0}^{q-2} \mathfrak{A}_{K^{(2)}/K}\varepsilon_i.$$

To determine the structure of $\mathfrak{D}^{(2)}$ over $\mathfrak{A}_{K^{(2)}/K}$ it is therefore sufficient to determine the structure of each $\varepsilon_i\mathfrak{D}^{(2)}$ over its associated order $\mathfrak{A}_i = \mathfrak{A}_{K^{(2)}/K}\varepsilon_i$ in $K\tilde{\Gamma}\varepsilon_i$.

The fields $K^{(n)}$ and the isomorphisms $(\mathfrak{o}/\pi^n\mathfrak{o})^\times \to \Gamma^{(n)}$ depend only on π and not on the Lubin–Tate series $f(X)$. Henceforth, without loss of generality, we take $f(X)$ to be the standard Lubin–Tate polynomial $\pi X + X^q$.

Fix $\omega = \omega_2 \in G^{(2)} \backslash G^{(1)}$ and set $\omega_1 = [\pi](\omega_2) \in G^{(1)} \backslash \{0\}$. Then

$$v_{K^{(2)}}(\omega) = 1, \qquad v_{K^{(2)}}(\omega_1) = q, \qquad v_{K^{(2)}}(\pi) = q(q-1). \tag{2.2}$$

Our choice of $f(X)$ ensures that

$$[\mu](X) = \mu X \qquad \text{if} \quad \mu^{q-1} = 1 \tag{2.3}$$

(see [4, Proposition 3.1]). Now

$$\sum_{\mu^{q-1}=1} \mu^m = \begin{cases} q-1 & \text{if} \quad m \equiv 0 \bmod (q-1); \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

Thus, using (2.1) and (2.3), one readily sees that

$$\varepsilon_i(\omega^j\omega_1^k) = \begin{cases} \omega^j\omega_1^k & \text{if} \quad j+k \equiv i \bmod (q-1); \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

Next, following [4], we set

$$\tau_h = \frac{1}{q-1} \sum_{\mu^{q-1}=1} \mu^{-h}(\langle 1+\pi\mu \rangle - 1) \in \mathfrak{o}\Gamma. \tag{2.6}$$

Thus τ_h depends only on $h \bmod (q-1)$, and the τ_h for $1 \leqslant h \leqslant q-1$ form an $\mathfrak{o}$-basis of $(\mathfrak{o}\Gamma)^+$. Also,

$$\tau_{q-1} = \frac{1}{q-1} \sum_{\gamma \in \Gamma \setminus \{1\}} (\gamma - 1) = \frac{1}{q-1} (T_\Gamma - q). \tag{2.7}$$

PROPOSITION 2.8. (i) $\tau_h(\varepsilon_i \mathfrak{O}^{(2)}) \subseteq \varepsilon_i \mathfrak{O}^{(2)}$ *for all* h, i;

(ii) $\tau_h(\omega^j) \equiv \binom{j}{h} \omega^{j-h} \omega_1^h \bmod \omega^{j+(q-1)h+1} \mathfrak{O}^{(2)}$ *for* $j \geqslant 0$ *and* $1 \leqslant h \leqslant q-1$.

Proof. (i) Since $\mathfrak{O}^{(2)}$ is a module over the commutative ring $\mathfrak{o}\tilde{\Gamma}$ we have $\tau_h \varepsilon_i(\mathfrak{O}^{(2)}) = \varepsilon_i(\tau_h \mathfrak{O}^{(2)}) \subseteq \varepsilon_i \mathfrak{O}^{(2)}$.

(ii) We argue as in [4]. Let

$$F(X, Y) = X + Y + \sum_{r, s \geqslant 1} c_{r,s} X^r Y^s$$

with $c_{r,s} \in \mathfrak{o}$. Then, because of our choice of $f(X)$, we have $c_{r,s} = 0$ when $r + s < q$ (see [4, Proposition 3.2(i)]). Thus

$$F(X, Y)^j - X^j = \sum_{s \geqslant 1} \binom{j}{s} X^{j-s} Y^s + \sum_{r, s \geqslant 1} b_{r,s} X^r Y^s \tag{2.9}$$

where $b_{r,s} \in \mathfrak{o}$, and $b_{r,s} = 0$ when $r + s < q + j - 1$. Using (2.3) and (2.9), we calculate

$$\begin{aligned}
(\langle 1 + \mu\pi \rangle - 1)(\omega^j) &= [1 + \mu\pi](\omega)^j - \omega^j \\
&= F(\omega, [\mu\pi](\omega))^j - \omega^j \\
&= F(\omega, \mu\omega_1)^j - \omega^j \\
&= \sum_{s \geqslant 1} \binom{j}{s} \omega^{j-s} (\mu\omega_1)^s + \sum_{r, s \geqslant 1} b_{r,s} \omega^r (\mu\omega_1)^s.
\end{aligned}$$

Hence, for $1 \leqslant h \leqslant q-1$, we have

$$\tau_h(\omega^j) = \frac{1}{q-1} \sum_{\mu^{q-1} = 1} \mu^{-h} \left(\sum_{s \geqslant 1} \binom{j}{s} \omega^{j-s} (\mu\omega_1)^s + \sum_{r, s \geqslant 1} b_{r,s} \omega^r (\mu\omega_1)^s \right).$$

Interchanging the order of summation, we find from (2.4) that the terms with $s < h$ cancel. Using (2.2), we then arrive at the congruence stated. ∎

We next define a family of $\mathfrak{o}$-lattices in $K\Gamma$. For $0 \leqslant i \leqslant q-2$, let

$$\mathfrak{L}_i = \mathrm{Span}_{\mathfrak{o}} \left\{ 1, \tau_1, ..., \tau_{q-2-i}, \frac{1}{\pi}\tau_{q-1-i}, ..., \frac{1}{\pi}\tau_{q-1} \right\} \tag{2.10}$$

where $\mathrm{Span}_{\mathfrak{o}}$ denotes the $\mathfrak{o}$-module spanned by the elements indicated. In particular,

$$\mathfrak{L}_0 = \mathfrak{o}\Gamma + \mathfrak{o}\left(\frac{1}{\pi} T_\Gamma\right), \qquad \mathfrak{L}_{q-2} = \mathfrak{o} + \frac{1}{\pi}(\mathfrak{o}\Gamma)^+. \tag{2.11}$$

LEMMA 2.12. *Let $0 \leqslant i \leqslant q-2$. Then $\mathfrak{L}_i$ is an $\mathfrak{o}\Gamma$-module isomorphic to $\varepsilon_i \mathfrak{D}^{(2)}$. More precisely, $\varepsilon_i \mathfrak{D}^{(2)} = \mathfrak{L}_i \cdot \beta$ for any $\beta \in \varepsilon_i \mathfrak{D}^{(2)}$ with $v_{K^{(2)}}(\beta) = qi + q - 1$.*

Proof. As $K^{(2)}$ is totally ramified over K, it follows from (2.2) and (2.5) that $(\omega^j)_{0 \leqslant j < q(q-1)}$ is an $\mathfrak{o}$-basis of $\mathfrak{D}^{(2)}$ and that $(\omega^{i+(q-1)k})_{0 \leqslant k < q}$ is an $\mathfrak{o}$-basis of $\varepsilon_i \mathfrak{D}^{(2)}$. Thus there exist elements $\beta \in \varepsilon_i \mathfrak{D}^{(2)}$ with $v_{K^{(2)}}(\beta) = qi + q - 1$. Indeed, $\beta = \omega^{i+(q-1)(i+1)}$ will do. Furthermore, any sequence $(x_h)_{0 \leqslant h < q}$ of elements of $\varepsilon_i K^{(2)}$ such that

$$\{ v_{K^{(2)}}(x_h) \mid 0 \leqslant h \leqslant q-1 \} = \{ i + (q-1)k \mid 0 \leqslant k \leqslant q-1 \} \tag{2.13}$$

is an $\mathfrak{o}$-basis for $\varepsilon_i \mathfrak{D}^{(2)}$. We claim that, for any β as in the statement of the lemma, the sequence

$$\beta, \tau_1(\beta), ..., \tau_{q-2-i}(\beta), \frac{1}{\pi}\tau_{q-1-i}(\beta), ..., \frac{1}{\pi}\tau_{q-1}(\beta) \tag{2.14}$$

satisfies (2.13). This will suffice to prove the lemma.

Set $j = qi + q - 1$. Then we may write

$$\beta = \sum_{k=0}^{q-1} b_k \omega^{j+k(q-1)} \tag{2.15}$$

with $b_k \in \mathfrak{o}$ and $b_0 \in \mathfrak{o}^\times$. By a result of Kummer [16, p. 24], the exact power of p dividing a binomial coefficient $\binom{a}{b}$ is the number of carries occurring in the base-p addition of b and $a-b$. In particular, since $j \equiv q-1 \bmod q$, this shows that $\binom{j}{h}$ is a p-adic unit if $1 \leqslant h \leqslant q-1$. Thus, by (2.15) and Proposition 2.8(ii), we have

$$v_{K^{(2)}}(\tau_h(\beta)) = v_{K^{(2)}}(\omega^{j-h}\omega_1^h) = j - h + qh = i + (q-1)(i+1+h).$$

Hence the elements (2.14) satisfy the condition (2.13), as required. ∎

Lemma 2.12 reduces the determination of the $\mathfrak{o}\tilde{\Gamma}$-module structure of $\mathfrak{D}^{(2)}$ to the investigation of the $\mathfrak{o}\Gamma$-modules $\mathfrak{L}_i$. To describe these, we will express the multiplication in $\mathfrak{o}\Gamma$ in terms of the τ_h. We first rewrite τ_h. Let $\gamma = \langle 1+\pi \rangle \in \Gamma$, and, more generally, set $\gamma^\alpha = \langle 1+\pi\alpha \rangle$ for all $\alpha \in \mathfrak{o}$. Thus the isomorphism $\mathfrak{o}/\pi\mathfrak{o} \to \Gamma$ may be written $(\alpha \bmod \pi\mathfrak{o}) \mapsto \gamma^\alpha$. Let $\chi\colon \mathfrak{o}^\times \to \mathfrak{o}^\times$ be given by $\chi(\alpha) = \mu$ where $\mu \equiv \alpha \bmod \pi\mathfrak{o}$ and $\mu^{q-1} = 1$. (Thus χ is the composition of the natural map $\mathfrak{o}^\times \twoheadrightarrow (\mathfrak{o}/\pi\mathfrak{o})^\times$ with the Teichmüller character.) Then

$$\tau_h = \frac{1}{q-1} \sum_{\mu^{q-1}=1} \mu^{-h}(\gamma^\mu - 1) = \frac{1}{q-1} \sum_{\alpha} \chi^{-h}(\alpha)(\gamma^\alpha - 1) \tag{2.16}$$

where, in the last sum, $\alpha \in \mathfrak{o}^\times$ runs over a set of representatives of $(\mathfrak{o}/\pi\mathfrak{o})^\times$. Using (2.4), it follows that

$$\gamma^\alpha - 1 = \sum_{h=1}^{q-1} \chi^h(\alpha)\, \tau_h \qquad \text{for} \quad \alpha \in \mathfrak{o}^\times. \tag{2.17}$$

As in [2], we may now evaluate the product $\tau_h \tau_k$ by mimicking the standard calculation of the product of Gauss sums for the finite field $\mathfrak{o}/\pi\mathfrak{o}$ (see e.g. [21, Lemma 6.2]). The group elements γ^α play the role of the additive character values in the Gauss sums. For $a, b \in \mathfrak{o}$ we write $a \sim b$ to denote that $a = ub$ for some $u \in \mathfrak{o}^\times$. Then

$$\tau_h \tau_k \sim \begin{cases} J_{h,k}\, \tau_{h+k} & \text{if} \quad h, k \not\equiv 0 \pmod{q-1}; \\ q\tau_k & \text{if} \quad h \equiv 0 \pmod{q-1}; \\ q\tau_h & \text{if} \quad k \equiv 0 \pmod{q-1}. \end{cases} \tag{2.18}$$

Here $J_{h,k}$ is the Jacobi sum

$$J_{h,k} = \sum_{\mu^{q-1}=1 \neq \mu} \chi^{-h}(\mu)\, \chi^{-k}(1-\mu).$$

Using the relation between Gauss sums and Jacobi sums [21, Lemma 6.2], together with the formula for the valuation of the Gauss sum formed with the character χ^{-h} in terms of the base-p digit-sum of h [21, Proposition 6.13], one can obtain the valuation of the $J_{h,k}$, as in [2, Corollary 4.3.]. Let $c(h,k)$ denote that number of carries in the base-p addition of h and k. Then the result may be expressed as follows:

PROPOSITION 2.19. *For $1 \leqslant h, k \leqslant q-2$, we have*

$$J_{h,k} \sim \begin{cases} 1 & \text{if} \quad h+k \equiv 0 \pmod{q-1}: \\ p^{c(h,k)} & \text{otherwise.} \end{cases}$$

We can now determine when $\mathfrak{L}_i$ is free over its associated order $\mathfrak{A}_i$.

LEMMA 2.20. *Suppose that K is ramified over $\mathbb{Q}_p$. Then*

(i) *for $0 \leqslant i < (q-1)/2$, the lattice $\mathfrak{L}_i$ is an order in $K\Gamma$. Thus $\mathfrak{A}_i = \mathfrak{L}_i$ and $\mathfrak{L}_i$ is a free $\mathfrak{A}_i$-module on the generator 1.*

(ii) *for $(q-1)/2 \leqslant i \leqslant q-2$, the lattice $\mathfrak{L}_i$ is not an order. Moreover, $\mathfrak{A}_i = \mathfrak{L}_{q-2-i}$ and $\mathfrak{L}_i$ is not free over $\mathfrak{A}_i$.*

Proof. We have $\tau_h \in \mathfrak{o}\Gamma$ for all h, and $\mathfrak{o}\Gamma \subset \mathfrak{L}_i$. We therefore see from (2.10) that $\mathfrak{L}_i$ will be an order if and only if

$$\left(\frac{1}{\pi}\tau_h\right)\left(\frac{1}{\pi}\tau_k\right) \in \mathfrak{L}_i \qquad \text{whenever} \quad q-1-i \leqslant h,k \leqslant q-1. \tag{2.21}$$

First let $0 \leqslant i < (q-1)/2$. It is immediate from (2.18) that the cases $h = q-1$ and $k = q-1$ of (2.21) hold, since π divides q. If $q-1-i \leqslant h$, $k \leqslant q-2$ then

$$\left(\frac{1}{\pi}\tau_h\right)\left(\frac{1}{\pi}\tau_k\right) \sim \pi^{-2} J_{h,k}\tau_{h+k}.$$

Here $J_{h,k}$ is divisible by p since a carry must occur in the base-p addition of h and k when $h+k \geqslant q$. But π^2 divides p since $K/\mathbb{Q}_p$ is ramified, so (2.21) again holds. This proves the first sentence of (i), and the second follows immediately.

Now let $(q-1)/2 \leqslant i \leqslant q-2$. Let $h = k = (q-1)/2$ if q is odd and $h = q/2-1$, $k = q/2$ if q is even. In either case,

$$\left(\frac{1}{\pi}\tau_h\right)\left(\frac{1}{\pi}\tau_k\right) \sim \pi^{-2} J_{h,k}\tau_{q-1}$$

with $J_{h,k} \sim 1$ since no carry can occur in base-p addition of h and k when $h+k = q-1$. Thus (2.21) fails and $\mathfrak{L}_i$ is not an order.

We next show that $\mathfrak{L}_{q-2-i} \cdot \mathfrak{L}_i \subseteq \mathfrak{L}_i$, or equivalently, that

$$\left(\frac{1}{\pi}\tau_h\right)\left(\frac{1}{\pi}\tau_k\right) \in \mathfrak{L}_i \qquad \begin{array}{l} \text{if} \quad i+1 \leqslant h \leqslant q-1 \\ \text{and} \quad q-1-i \leqslant k \leqslant q-1. \end{array} \tag{2.22}$$

For $h = q-1$ and $h, k \leqslant q-2$, this follows exactly as in the proof of (2.21) for $i < (q-1)/2$. In the remaining case $k = q-1$, we have

$$\left(\frac{1}{\pi}\tau_h\right)\left(\frac{1}{\pi}\tau_k\right) \sim (\pi^{-2}q)\,\tau_h \in \mathfrak{L}_i,$$

again using the fact that $K/\mathbb{Q}_p$ is ramified. Hence $\mathfrak{L}_{q-2-i} \cdot \mathfrak{L}_i \subseteq \mathfrak{L}_i$.

We have now shown that $\mathfrak{L}_{q-2-i} \subseteq \mathfrak{A}_i$. To establish the reverse inclusion, suppose that

$$\xi = a_0 + \sum_{h=1}^{i} a_h \tau_h + \sum_{h=i+1}^{q-1} a_h \frac{1}{\pi}\tau_h \in \mathfrak{A}_i$$

with $a_h \in K$ for all h. We claim that in fact $a_h \in \mathfrak{o}$ for all h. For $0 \leqslant h \leqslant q-2-i$ and for $i+1 \leqslant h \leqslant q-1$, this is clear since $\xi = \xi \cdot 1 \in \mathfrak{L}_i$. For $q-1-i \leqslant h \leqslant i$, consideration of the coefficient of $\pi^{-1}\tau_{q-1}$ in $\xi \cdot (\pi^{-1}\tau_{q-1-h})$ shows that $a_h \in \mathfrak{o}$, again using that $J_{h,k} \sim 1$ when $h+k = q-1$. Thus the claim holds, and it follows that $\xi \in \mathfrak{L}_{q-2-i}$. We have now shown that $\mathfrak{A}_i = \mathfrak{L}_{q-2-i}$.

Finally, we show that $\mathfrak{L}_i$ cannot be a free $\mathfrak{L}_i$-module. Let $\lambda \in \mathfrak{L}_i$. Then

$$\tau_i \cdot \lambda \in \mathfrak{o}\left(\frac{1}{\pi}\tau_{q-1}\right) + \pi\mathfrak{L}_i. \tag{2.23}$$

Indeed, it is enough to verify this with λ running through the basis elements of $\mathfrak{L}_i$ listed in (2.10). Clearly $\tau_i \cdot 1 = 0$. For $1 \leqslant h \leqslant q-2-i$, we have $\tau_i \cdot \tau_h \in \mathfrak{o}\tau_{i+h} \subset \pi\mathfrak{L}_i$, the last inclusion holding since $i+h > i \geqslant q-1-i$. For $h = q-1-i$, we have $\tau_i \cdot (\pi^{-1}\tau_h) \sim \pi^{-1}\tau_{q-1}$. For $q-i \leqslant h \leqslant q-1$, we have $\tau_i \cdot (\pi^{-1}\tau_h) \in \pi^{-1}p\,\mathfrak{o}\Gamma \subset \pi\mathfrak{L}_i$ since $J_{i,h}$ is divisible by p when $i+h \geqslant q$, and $K/\mathbb{Q}_p$ is ramified. This establishes (2.23). Directly from (2.10) and (2.18), we have

$$\left(\frac{1}{\pi}\tau_{q-1}\right) \cdot \lambda \in \mathfrak{o}\left(\frac{1}{\pi}\tau_{q-1}\right) + \pi\mathfrak{L}_i. \tag{2.24}$$

Now (2.23) and (2.24) show that the images in $\mathfrak{L}_i/\pi\mathfrak{L}_i$ of $\tau_i \cdot \lambda$ and $(\pi^{-1}\tau_{q-1}) \cdot \lambda$ are not linearly independent over $\mathfrak{o}/\pi\mathfrak{o}$. As τ_i and $\pi^{-1}\tau_{q-1}$ are elements of the basis (2.10) of $\mathfrak{A}_i = \mathfrak{L}_{q-2-i}$, it follows that λ cannot be a free generator of the $\mathfrak{A}_i$-module $\mathfrak{L}_i$. But $\lambda \in \mathfrak{L}_i$ is arbitrary, so $\mathfrak{L}_i$ is not free as an $\mathfrak{A}_i$-module. ∎

For any elementary abelian p-group Δ, we define $\mathfrak{o}$-lattices

$$\mathfrak{L}_*(\Delta) = \mathfrak{o}\Delta + \mathfrak{o}\left(\frac{1}{\pi}T_\Delta\right) \qquad \text{and} \qquad \mathfrak{L}^*(\Delta) = \mathfrak{o}\,\frac{1}{\pi}(\mathfrak{o}\Delta)^+ \tag{2.25}$$

in $K\Delta$. Thus by (2.11), $\mathfrak{L}_0 = \mathfrak{L}_*(\Gamma)$ and $\mathfrak{L}_{q-2} = \mathfrak{L}^*(\Gamma)$. We note the following consequence of the proof of Lemma 2.20:

COROLLARY 2.26. *Let Δ be an elementary abelian p-group. Then*

(i) *$\mathfrak{L}_*(\Delta)$ is an order in $K\Delta$, and hence $\mathfrak{L}_*(\Delta) = \mathfrak{o}\Delta[(1/\pi)\, T_\Delta]$.*

(ii) *$\mathfrak{L}^*(\Delta)$ has associated order $\mathfrak{L}_*(\Delta)$. Moreover, if K is ramified over $\mathbb{Q}_p$ and $|\Delta| > 2$, then $\mathfrak{L}_*(\Delta)$ is not free over $\mathfrak{L}_*(\Delta)$.*

Proof. First let $\Delta = \Gamma$. In the proof of Lemma 2.20, the only case of (2.21) when $i = 0$ is $h = k = q-1$, and the only case of (2.22) when $i = q-2$ is $h = q-1$. Thus the hypothesis that $K/\mathbb{Q}_p$ is ramified was not used in the case $i = 0$, and was used in the case $i = q-2$ only to show that $\mathfrak{L}_{q-2}$ is not free over $\mathfrak{L}_0$. Thus the Corollary holds for $\Delta = \Gamma$.

Now let E be an unramified extension of K. The proof of Lemma 2.20 goes through after extending scalars from $\mathfrak{o}$ to $\mathfrak{O}_E$, so the analogous statements to (i), (ii) hold for $\mathfrak{L}_*(\Gamma) \otimes_{\mathfrak{o}} \mathfrak{O}_E$ and $\mathfrak{L}^*(\Gamma) \otimes_{\mathfrak{o}} \mathfrak{O}_E$. We can then replace Γ by Δ, provided that E is chosen so that the residue field of $\mathfrak{O}_E$ has a subfield of cardinality $|\Delta|$. It is then clear from (2.25) that the result descends to $\mathfrak{o}$. ∎

Unlike the lattices $\mathfrak{L}_i$ in general, $\mathfrak{L}_*(\Gamma)$ and $\mathfrak{L}^*(\Gamma)$ behave nicely under the operation of taking fixed points for a subgroup of Γ. Indeed, as is readily checked, we have

PROPOSITION 2.27. *Let $\Gamma = \Sigma \times \Delta$ be an elementary abelian p-group. Then $\mathfrak{L}_*(\Gamma)^\Sigma = \mathfrak{L}_*(\Delta)\, T_\Sigma$ and $\mathfrak{L}^*(\Gamma)^\Sigma = \mathfrak{L}^*(\Delta)\, T_\Sigma$.*

Proof of Theorem 1. Let d be a divisor of $q-1$, say with $rd = q-1$. Then

$$L_d = \bigoplus_{k=0}^{r-1} \varepsilon_{kd} K^{(2)}.$$

Hence

$$\mathfrak{O}_{L_d} = \bigoplus_{k=0}^{r-1} \varepsilon_{kd} \mathfrak{O}^{(2)} \qquad \text{and} \qquad \mathfrak{A}_{L_d/K} = \bigoplus_{k=0}^{r-1} \mathfrak{A}_{kd} \varepsilon_{kd}.$$

Thus $\mathfrak{O}_{L_d}$ is free over $\mathfrak{A}_{L_d/K}$ if and only if each $\varepsilon_{kd}\mathfrak{O}^{(2)}$ is free over $\mathfrak{A}_{kd}$.

If $d = q-1$ then $\mathfrak{O}_{L_d} = \mathfrak{O}' = \varepsilon_0 \mathfrak{O}^{(2)}$. Now by Lemma 2.12, $\varepsilon_0 \mathfrak{O}^{(2)} = \mathfrak{L}_0 \cdot \beta$ for any $\beta \in \varepsilon_0 \mathfrak{O}^{(2)}$ with $v_{K^{(2)}}(\beta) = q-1$, and by Corollary 2.26(i), $\mathfrak{L}_0$ is free over $\mathfrak{o}\Gamma[\pi^{-1} T_\Gamma]$ (whether or not $K/\mathbb{Q}_p$ is ramified). This proves Theorem 1(i).

If $d \neq q-1$ then $(r-1)\,d \geqslant (q-1)/2$. When $K/\mathbb{Q}_p$ is ramified, it follows from Lemmas 2.12 and 2.20(ii) that $\varepsilon_{(r-1)\,d}\mathfrak{O}^{(2)}$ is not free over $\mathfrak{A}_{(r-1)\,d} = \mathfrak{L}_{d-1}$, and hence that $\mathfrak{O}_{L_d}$ is not free over $\mathfrak{A}_{L_d/K}$. This proves Theorem 1(ii). ∎

From the above proof and Lemma 2.20, we can extract an explicit description of the associated orders.

COROLLARY 2.28. *Suppose that $K/\mathbb{Q}_p$ is ramified, and let $q-1 = rd$. Then*

$$\mathfrak{A}_{L_d/K} = \bigoplus_{\substack{0 \leqslant i < (q-1)/2 \\ i \equiv 0 \bmod d}} \mathfrak{L}_i \varepsilon_i \oplus \bigoplus_{\substack{(q-1)/2 \leqslant i \leqslant q-2 \\ i \equiv 0 \bmod d}} \mathfrak{L}_i \varepsilon_{q-2-i}.$$

In particular,

$$\mathfrak{A}_{K^{(2)}/K} = \bigoplus_{0 \leqslant i < (q-1)/2} \mathfrak{L}_i \varepsilon_i \oplus \bigoplus_{(q-1)/2 \leqslant i \leqslant q-2} \mathfrak{L}_i \varepsilon_{q-2-i}.$$

If r is even then exactly half of the summands $\varepsilon_i \mathfrak{O}^{(2)}$ occurring in $\mathfrak{O}_{L_d}$ are free over their associated orders. If r is odd, then $(r+1)/2$ of the summands are free and $(r-1)/2$ are not free. In particular, if q is odd then exactly half the summands occurring in $\mathfrak{O}^{(2)}$ are free, and if q is even then $q/2$ of the summands occurring in $\mathfrak{O}^{(2)}$ are free and $(q/2)-1$ are not free.

3. INTERMEDIATE FIELDS OF K'/K AND $K^{(2)}/K^{(1)}$

We next deduce Theorems 2 and 3, dealing with the fields on the vertical edges of the parallelogram of Fig. 2. In this section and the next, we shall make use of local class field theory and of ramification theory, in particular the transition between the ramification groups Γ_u in the lower numbering and Γ^v in the upper numbering. The results we need can be found in [17] and [12, Section 9].

Let Σ be a subgroup of Γ, and let F (respectively F') be the subfield of $K^{(2)}$ (respectively, K') fixed by Σ. Since Γ is elementary abelian, we may choose a subgroup Δ of Γ so that $\Gamma = \Sigma \times \Delta$. We identify Δ by restriction with $\mathrm{Gal}(F/K^{(1)}) = \Gamma/\Sigma$ and also with $\mathrm{Gal}(F'/K)$.

LEMMA 3.1. *In the notation of* (2.25), *we have $\mathfrak{O}_{F'} \cong \mathfrak{L}_*(\Delta)$ and $\varepsilon_{q-2}\mathfrak{O}_F \cong \mathfrak{L}^*(\Delta)$ as $\mathfrak{o}\Delta$-modules. In fact, $\mathfrak{O}_{F'} = \mathfrak{L}_*(\Delta)\cdot\beta$ for any $\beta \in \mathfrak{O}_{F'}$ with $v_{F'}(\beta) = 1$.*

Proof. Since $\varepsilon_0\mathfrak{O}^{(2)}=\mathfrak{O}'$ and $K^{(2)}/K'$ is totally ramified of degree $q-1$, Lemma 2.12 shows that $\mathfrak{O}'=\mathfrak{L}_0\cdot\beta_0=\mathfrak{L}_*(\Gamma)\cdot\beta_0$ for any $\beta_0\in\mathfrak{O}'$ with $v_{K'}(\beta_0)=1$. Taking fixed points under Σ, we have

$$\mathfrak{O}_{F'}=\mathfrak{O}'^{\Sigma}=(\mathfrak{L}_*(\Gamma)\cdot\beta_0)^{\Sigma}=(\mathfrak{L}_*(\Gamma)^{\Sigma})\cdot\beta_0=\mathfrak{L}_*(\Delta)\cdot(T_\Sigma\cdot\beta_0),$$

using Proposition 2.27. This shows that $\mathfrak{O}_{F'}\cong\mathfrak{L}_*(\Delta)$. Similarly,

$$\varepsilon_{q-2}\mathfrak{O}_F=(\varepsilon_{q-2}\mathfrak{O}_K)^{\Sigma}\cong\mathfrak{L}^*(\Gamma)^{\Sigma}=\mathfrak{L}^*(\Delta)\cdot T_\Sigma\cong\mathfrak{L}^*(\Delta).$$

It remains to show that every $\beta\in\mathfrak{O}_{F'}$ with $v_{F'}(\beta)=1$ can be written as $\beta=T_\Sigma\cdot\beta_0$ for some $\beta_0\in\mathfrak{O}'$ with $v_{K'}(\beta_0)=1$. Let $\mathrm{Tr}\colon K'\to F'$ denote the trace, and let $\mathfrak{P}_{K'}$, $\mathfrak{P}_{F'}$ denote the maximal ideals of $\mathfrak{O}'$, $\mathfrak{O}_{F'}$ respectively. It will suffice to show that

$$\mathrm{Tr}(\mathfrak{P}_{K'})=\mathfrak{P}_{F'}\qquad\text{and}\qquad\mathrm{Tr}(\mathfrak{P}_{K'}^2)=\mathfrak{P}_{F'}^2. \tag{3.2}$$

From [17, p. 157] we know that the ramification jumps of the extension $K^{(2)}/K$ occur at $v=0,1$ in the upper numbering. It follows using Herbrand's theorem that the p-extension K'/K has a unique jump, occurring at 1 in the upper (and hence also the lower) numbering. The same is therefore true of K'/F'. By Hilbert's formula [12, Proposition 4 on p. 36], the inverse different $\mathfrak{D}^{-1}$ of K'/F' is then $\mathfrak{P}_{K'}^{2-2p^f}$ where $p^f=[K':F']$. If $\mathfrak{P}_{K'}^a$ is any $\mathfrak{O}'$-ideal then $\mathrm{Tr}(\mathfrak{P}_{K'}^a)$ is the smallest $\mathfrak{O}_{F'}$-ideal $\mathfrak{P}_{F'}^b$ for which $\mathfrak{P}_{K'}^a\mathfrak{P}_{F'}^{-b}=\mathfrak{P}_{K'}^{a-p^fb}\subseteq\mathfrak{D}^{-1}$. Taking $a=1$ and $a=2$, we obtain (3.2). ∎

Proof of Theorem 2. From Lemma 3.1 and Corollary 2.26(i), we have

$$\mathfrak{O}_{F'}=\mathfrak{o}\Delta\left[\frac{1}{\pi}T_\Delta\right]\cdot\beta$$

for any $\beta\in F'$ with $v_{F'}(\beta)=1$. Thus $\mathfrak{O}_{F'}$ is free on the generator β over the order $\mathfrak{o}\Delta[\pi^{-1}T_\Delta]$, which therefore coincides with $\mathfrak{A}_{F'/K}$. ∎

Proof of Theorem 3. We have

$$\mathfrak{O}_F=(\mathfrak{O}^{(2)})^{\Sigma}=\bigoplus_{i=0}^{q-2}(\varepsilon_i\mathfrak{O}^{(2)})^{\Sigma}=\bigoplus_{i=0}^{q-2}\varepsilon_i\mathfrak{O}_F.$$

For $\mathfrak{O}_F$ to be free over $\mathfrak{A}_{F/K}$ we therefore require each summand $\varepsilon_i\mathfrak{O}_F$ to be free over its associated order in $K\Delta$. Now $\varepsilon_{q-2}\mathfrak{O}_F\cong\mathfrak{L}^*(\Delta)$ by Lemma 3.1. By Corollary 2.26(ii) this summand is not free over its associated order, since $|\Delta|>2$ by hypothesis. ∎

4. WEAKLY RAMIFIED EXTENSIONS

Before considering fields corresponding to interior points of the parallelogram of Fig. 2, we pause to derive Theorem 5 from Theorem 2.

Up to now we have been considering subfields of $K^{(2)}$, the Lubin–Tate division field corresponding to a fixed uniformising parameter π of K. In this section, we allow π to vary. We therefore write $K_\pi^{(n)}$ for the nth Lubin–Tate division field of K corresponding to π.

We begin with a general result about totally ramified abelian extensions of K.

PROPOSITION 4.1. *Let F be a finite totally ramified abelian extension of K. Then $F \subseteq K_\pi^{(n)}$ for some uniformising parameter π and some $n \geqslant 1$.*

Proof. Let $N: F \to K$ be the norm. By local class field theory, $N(F^\times)$ is an open subgroup of $K^\times$ containing some uniformising parameter π. Thus $N(F^\times)$ contains the subgroup generated by π and $1 + \pi^n \mathfrak{o}$ for large enough n. This subgroup has $K_\pi^{(n)}$ as its class field, so $F \subseteq K_\pi^{(n)}$. ∎

LEMMA 4.2. *Let F be a totally ramified abelian extension of K of degree $p^f d$, where d is prime to p. Suppose that F is weakly ramified over K. Then $d = 1$ and $F \subseteq K_\pi^{(2)}$ for some uniformising parameter π.*

Proof. Let $\Delta = \mathrm{Gal}(F/K)$. Then $|\Delta_0| = |\Delta| = p^f d$, $|\Delta_1| = p^f$, and $|\Delta_2| = 1$. Thus the last jump in the ramification filtration comes at $u = 1$ in the lower numbering, and hence at $v = \phi(1) = d^{-1}$ in the upper numbering. Here ϕ is the Herbrand function (see [17, p. 155]). By the Hasse–Arf theorem [17, p. 157], the jumps in the upper numbering must occur at integral values of v, so $d = 1$.

By Proposition 4.1, $F \subseteq K_\pi^{(n)}$ for some π and some n. We may certainly assume that $n \geqslant 2$, and we have to prove that we can take $n = 2$. Let $\Gamma = \mathrm{Gal}(K_\pi^{(n)}/K)$ and $\Sigma = \mathrm{Gal}(K_\pi^{(n)}/F)$. By Herbrand's theorem, we then have $(\Gamma^v \Sigma)/\Sigma = \Delta^v = \{1\}$ for all $v > 1$, so in particular $\Gamma^2 \subseteq \Sigma$. Since $\Gamma^2 = \mathrm{Gal}(K_\pi^{(n)}/K_\pi^{(2)})$, it follows that $F \subseteq K_\pi^{(2)}$ as required. ∎

This allows us to deduce a special case of Theorem 5.

COROLLARY 4.3. *Let F be a totally ramified abelian extension of K, and set $\Delta = \mathrm{Gal}(F/K)$. If F/K is weakly ramified then $\mathfrak{A}_{F/K} = \mathfrak{o}\Delta[\pi^{-1} T_\Delta]$ and $\mathfrak{O}_F$ is free over $\mathfrak{A}_{F/K}$.*

Proof. Choose π as in Lemma 4.2. As before, let $\tilde{\Gamma} = \mathrm{Gal}(K^{(2)}/K)$, so $\tilde{\Gamma} = \Gamma \times \Gamma^{(1)}$ where Γ has order q and $\Gamma^{(1)}$ has order $q - 1$. Since $F \subseteq K_\pi^{(2)}$ and F/K is a p-extension, we have $F \subseteq K' = (K^{(2)})^{\Gamma^{(1)}}$. The result then follows from Theorem 2. ∎

It remains to remove the hypothesis that F/K is totally ramified. We write $e(N/L)$ for the ramification index of an extension N/L.

PROPOSITION 4.4. *Let $L \subseteq M$ be finite normal extensions of K with M/L unramified. Let $\Gamma = \mathrm{Gal}(M/K)$ and $\Delta = \mathrm{Gal}(L/K)$. Then the natural map $\Gamma \twoheadrightarrow \Delta$ induces isomorphisms $\Gamma_i \cong \Delta_i$ for all $i \geqslant 0$. In particular, M/K is weakly ramified if and only if L/K is.*

Proof. Since M/L is unramified, we have $\mathrm{Gal}(M/L) \cap \Gamma_0 = \{1\}$, and the natural map induces an injection $\Gamma_0 \to \Delta_0$. This is an isomorphism since

$$|\Gamma_0| = e(M/K) = e(M/L)\, e(L/K) = e(L/K) = |\Delta_0|.$$

Let v be a uniformising parameter of L, and hence also of M, and let $\mathfrak{P}_L$, $\mathfrak{P}_M$ be the maximal ideals of $\mathfrak{O}_L$, $\mathfrak{O}_M$ respectively. For $\gamma \in \Gamma_0$, let $\bar{\gamma}$ denote the image of γ in Δ_0. Then for $i \geqslant 0$ we have

$$\begin{aligned} \bar{\gamma} \in \Delta_i &\Leftrightarrow (\bar{\gamma} - 1)\, v \in \mathfrak{P}_L^{i+1} \\ &\Leftrightarrow (\gamma - 1)\, v \in \mathfrak{P}_M^{i+1} \\ &\Leftrightarrow \gamma \in \Gamma_i. \end{aligned}$$

Thus Γ_i and Δ_i are isomorphic under the map $\gamma \mapsto \bar{\gamma}$. In particular, $\Gamma_2 = \{1\}$ if and only if $\Delta_2 = \{1\}$. ∎

Proof of Theorem 5. Given a weakly ramified abelian extension F/K, let $\bar{K}$ be the unramified extension of K of degree $[F : K]$, and set $\bar{F} = \bar{K}F$. By [14, Lemma 1], there is a field $F' \subseteq \bar{F}$ such that F'/K is totally ramified and $F'K = \bar{F}$. The various fields are indicated in Fig. 3, where the edges marked (t) represent totally ramified extensions, and all other edges represent unramified extensions.

As $\bar{F}/F$ and $\bar{F}/F'$ are unramified, we may apply Proposition 4.4 twice to show that $\bar{F}/K$, and then F'/K, are weakly ramified. Thus, by Corollary 4.3, $\mathfrak{O}_{F'}$ is free over its associated order $\mathfrak{A}_{F'/K} = \mathfrak{o}\Delta'[\pi^{-1}T_{\Delta'}]$, where $\Delta' = \mathrm{Gal}(F'/K)$. Now let $\Sigma = \mathrm{Gal}(\bar{K}/K)$. Since $\bar{K}/K$ is unramified, we have $\mathfrak{O}_{\bar{F}} = \mathfrak{O}_{F'} \otimes_{\mathfrak{o}} \mathfrak{O}_{\bar{K}}$, and $\mathfrak{O}_{\bar{K}}$ is free over $\mathfrak{A}_{\bar{K}/K} = \mathfrak{o}\Sigma$. Hence $\mathfrak{O}_{\bar{F}}$ is free over $\mathfrak{A}_{\bar{F}/K} = \mathfrak{o}\Delta'[\pi^{-1}T_{\Delta'}] \otimes \mathfrak{o}\Sigma$.

Finally, let $\Gamma = \mathrm{Gal}(\bar{F}/K)$. We may identify Γ with $\Delta' \times \Sigma$. Since $\bar{F}/F$ is unramified, it follows from [6, Lemma 6] that $\mathfrak{O}_F$ is free over $\mathfrak{A}_{F/K}$, and that this order is the image of $\mathfrak{A}_{\bar{F}/K}$ under the natural map $\Gamma \twoheadrightarrow \Delta = \mathrm{Gal}(F/K)$. By Proposition 4.4, this takes $\Gamma_0 = \Delta'$ to Δ_0, so we have $\mathfrak{A}_{F/K} = \mathfrak{o}\Delta[\pi^{-1}T_{\Delta_0}]$. ∎

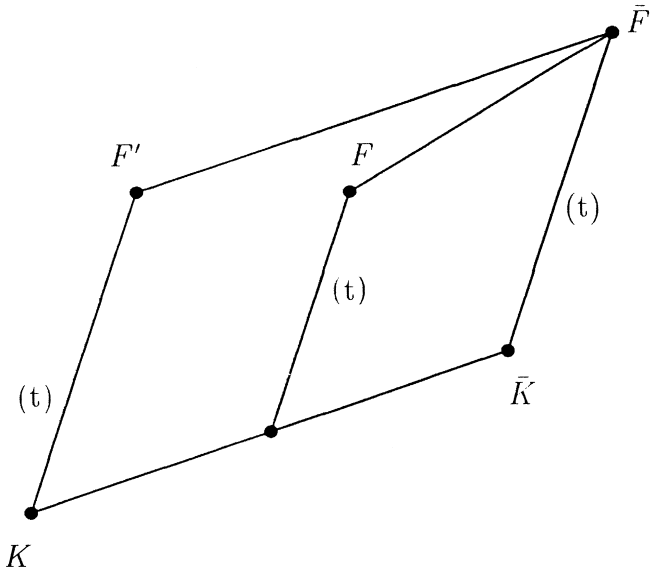

FIG. 3. Fields occurring in the proof of Theorem 5.

5. INTERIOR FIELDS

We now return to the situation of Sections 2 and 3. Recall that K is an extension of $\mathbb{Q}_p$ with uniformising parameter π. We identify the residue field $\mathfrak{o}/\pi\mathfrak{o}$ with the finite field $\mathbb{F}_q$ of cardinality q. The field $K^{(1)}$ (respectively, $K^{(2)}$) is the first (respectively, second) Lubin–Tate division field of K relative to π. The (multiplicative) group $\Gamma = \mathrm{Gal}(K^{(2)}/K^{(1)})$ is identified with the additive group of $\mathbb{F}_q$ via $\alpha \mapsto \langle 1 + \pi\alpha \rangle$ for $\alpha \in \mathbb{F}_q$.

In this section, we investigate the integral Galois module structure of certain fields in the interior of the parallelogram of Fig. 2. In particular, we shall prove Theorem 4. Dealing with an arbitrary interior field would, by Lemma 2.12, be tantamount to describing the fixed-point lattices $\mathfrak{L}_i^{\Sigma}$ for an arbitrary subgroup Σ of Γ. Here $\mathfrak{L}_i^{\Sigma}$ is naturally an $\mathfrak{o}\bar{\Delta}$-module, where $\bar{\Delta} = \Gamma/\Sigma$. Recall that $\mathfrak{L}_i$ is defined in terms of the elements τ_h of (2.6), whose definition involves the multiplicative structure of $\mathbb{F}_q$ via the factor μ^{-h}. In general, $\bar{\Delta}$ does not inherit the structure of a finite field, so it is unreasonable to expect an explicit description of $\mathfrak{L}_i^{\Sigma}$ along the lines of (2.10). We can however obtain such a description in the special case where $\bar{\Delta}$ becomes a vector space of dimension 1 over a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$. This is what enables us to prove Theorem 4.

We shall require a result on certain sums in $\mathbb{F}_q$. Let V be an $\mathbb{F}_{q_0}$-subspace of $\mathbb{F}_q$. For any $\alpha \in \mathbb{F}_q$ and any integer $h \geqslant 0$, define

$$S_h(V; \alpha) = \sum_{v \in V} (v + \alpha)^h. \tag{5.1}$$

In [5] we give several results on the vanishing or otherwise of the sums $S_h(V; \alpha)$. In particular, from [5, Theorem 3(iv)] we have the following result:

LEMMA 5.2. *Let V have dimension m over $\mathbb{F}_{q_0}$ and let $0 \leqslant k \leqslant q_0 - 2$. Then*

(i) $S_h(V; \alpha) = 0$ *if* $0 \leqslant h \leqslant (k+1)\, q_0^m - 2$ *and* $h \equiv k \bmod (q_0 - 1)$;

(ii) $S_{(k+1)\, q_0^m - 1}(V; \alpha) = 0$ *if and only if* $k \neq 0$ *and* $\alpha \in V$.

Now let Σ be a subgroup of Γ corresponding to an $\mathbb{F}_{q_0}$-subspace V of $\mathbb{F}_q$ of codimension 1. Let V have dimension m over $\mathbb{F}_{q_0}$ (so $q = q_0^{m+1}$). To avoid trivialities, we assume that $q_0 \neq q$. Let Δ be a subgroup of Γ corresponding to a subspace $W = \mathbb{F}_{q_0} w$ of $\mathbb{F}_q$ complementary to V. Then, setting $\delta = \gamma^w$, we have $\Delta = \{\delta^\alpha \mid \alpha \in \mathbb{F}_{q_0}\}$ and $\Gamma = \Sigma \times \Delta$. We may therefore identify Δ with $\overline{\Delta} = \Gamma / \Sigma$.

Analogously to (2.16) and (2.10) we define

$$\tau_k^{(\Delta)} = \frac{1}{q_0 - 1} \sum_{\alpha \in \mathbb{F}_{q_0}^\times} \chi^{-k}(\alpha)(\delta^\alpha - 1) \in \mathfrak{o}\Delta$$

for $1 \leqslant k \leqslant q_0 - 1$, and

$$\mathfrak{Q}_j(\Delta) = \mathrm{Span}_{\mathfrak{o}} \left\{ 1, \tau_1^{(\Delta)}, \ldots, \tau_{q_0 - 2 - j}^{(\Delta)}, \frac{1}{\pi} \tau_{q_0 - 1 - j}^{(\Delta)}, \ldots, \frac{1}{\pi} \tau_{q_0 - 1}^{(\Delta)} \right\}$$

for $0 \leqslant j \leqslant q_0 - 2$.

For each of the lattices $\mathfrak{Q}_i$ of (2.10) we must determine the fixed-point lattice $\mathfrak{Q}_i^\Sigma$. Clearly

$$\mathfrak{Q}_i^\Sigma = \mathfrak{Q}_i \cap (K\Delta)\, T_\Sigma, \tag{5.3}$$

and since $\mathfrak{Q}_0 \subseteq \mathfrak{Q}_i \subseteq \mathfrak{Q}_{q-2}$, it follows from Proposition 2.27 that

$$\mathfrak{Q}_0(\Delta)\, T_\Sigma \subseteq \mathfrak{Q}_i^\Sigma \subseteq \mathfrak{Q}_{q_0 - 2}(\Delta)\, T_\Sigma \qquad \text{for} \quad 0 \leqslant i \leqslant q - 2. \tag{5.4}$$

In particular,

$$\frac{1}{\pi} \tau_{q_0 - 1}^{(\Delta)} T_\Sigma \in \mathfrak{Q}_i^\Sigma \qquad \text{for all } i. \tag{5.5}$$

LEMMA 5.6. *Let* $0 \leqslant i \leqslant q-2$. *Then* $\mathfrak{L}_i^{\Sigma} = \mathfrak{L}_{j(i)}(\Delta)\, T_{\Sigma}$ *where*

$$j(i) = \begin{cases} \lfloor i/q_0^m \rfloor & \text{if} \quad i < q_0^m(q_0-1); \\ q_0-2 & \text{if} \quad i \geqslant q_0^m(q_0-1). \end{cases} \tag{5.7}$$

Thus when $0 \leqslant j \leqslant q_0-3$, *we have* $\mathfrak{L}_i^{\Sigma} = \mathfrak{L}_j(\Delta)\, T_{\Sigma}$ *for* $q_0^m j \leqslant i \leqslant q_0^m(j+1) - 1$, *while* $\mathfrak{L}_i^{\Sigma} = \mathfrak{L}_{q_0-2}(\Delta)\, T_{\Sigma}$ *for* $q_0^m(q_0-2) \leqslant i \leqslant q-2$.

Proof. We first express the products $\tau_k^{(\Delta)} T_{\Sigma}$ for $1 \leqslant k \leqslant q_0-1$ in terms of the basis elements τ_h of $\mathfrak{o}\Gamma^+$. Using (2.17), we calculate

$$\begin{aligned} (q_0-1)\, \tau_k^{(\Delta)} T_{\Sigma} &= \sum_{\alpha \in \mathbb{F}_{q_0}^{\times}} \chi^{-k}(\alpha)(\delta^{\alpha}-1) \sum_{v \in V} \gamma^v \\ &= \sum_{\alpha \in \mathbb{F}_{q_0}^{\times}} \sum_{v \in V} \chi^{-k}(\alpha)((\gamma^{w\alpha+v}-1)-(\gamma^v-1)) \\ &= \sum_{\alpha \in \mathbb{F}_{q_0}^{\times}} \sum_{v \in V} \chi^{-k}(\alpha) \sum_{h=0}^{q-1} (\chi^h(w\alpha+v)-\chi^h(v))\, \tau_h \\ &= \sum_{h=1}^{q-1} \left(\sum_{\alpha \in \mathbb{F}_{q_0}^{\times}} \chi^{h-k}(\alpha) \right) \left(\sum_{v \in V} (\chi^h(w+v)-\chi^h(v)) \right) \tau_h. \end{aligned}$$

(In the last line we have substituted αv for v.) The sum over α vanishes unless $h \equiv k \bmod (q_0-1)$. Thus, setting

$$S'_h = \sum_{v \in V} (\chi^h(w+v)-\chi^h(v)),$$

we have shown that

$$\tau_k^{(\Delta)} T_{\Sigma} = \sum_{h \equiv k \bmod (q_0-1)} S'_h \tau_h. \tag{5.8}$$

Let $1 \leqslant k \leqslant q_0-2$. It follows from (5.8) and (2.10) that $\pi^{-1}\tau_k^{(\Delta)} T_{\Sigma} \in \mathfrak{L}_i$ if and only if $S'_h \equiv 0 \bmod \pi\mathfrak{o}$ for all $h < q-1-i$ with $h \equiv k \bmod (q_0-1)$. We will simplify this condition using Lemma 5.2. In the notation of (5.1), the image of S'_h in $\mathfrak{o}/\pi\mathfrak{o} = \mathbb{F}_q$ is $S_h(V; w) - S_h(V; 0)$. Thus if $h \equiv k \bmod (q_0-1)$ and $h < (k+1)\, q_0^m - 1$ then $S'_h \equiv 0 \bmod \pi\mathfrak{o}$ by Lemma 5.2(i). If, however, $h = (k+1)\, q_0^m - 1$ then $S_h(V; 0) = 0$ but $S_h(V; w) \neq 0$ by Lemma 5.2(ii), so $S'_{(k+1)\, q^{m_0}-1} \not\equiv 0 \bmod \pi\mathfrak{o}$. It follows that

$$\frac{1}{\pi}\, \tau_k^{(\Delta)} T_{\Sigma} \in \mathfrak{L}_i^{\Sigma} \Leftrightarrow q-1-i \leqslant (k+1)\, q_0^m - 1$$

$$\Leftrightarrow q_0-1-k \leqslant \left\lfloor \frac{i}{q_0^m} \right\rfloor.$$

Taking into account (5.5) and (5.4), we have now shown that if $i < q_0^m(q_0-1)$ then the elements

$$T_\Sigma, (\tau_1^{(\Delta)} T_\Sigma), ..., (\tau_{q_0-2-j(i)}^{(\Delta)} T_\Sigma), \left(\frac{1}{\pi}\tau_{q_0-1-j(i)}^{(\Delta)} T_\Sigma\right), ..., \left(\frac{1}{\pi}\tau_{q_0-1}^{(\Delta)} T_\Sigma\right) \qquad (5.9)$$

lie in $\mathfrak{Q}_i^\Sigma \backslash \pi \mathfrak{Q}_i^\Sigma$. By (5.8), each τ_h occurs in $\tau_k^{(\Delta)} T_\Sigma$ for only one value of k, namely that for which $h \equiv k \bmod (q_0-1)$. It then follows from (2.10) and (5.4) that the elements (5.9) form a basis for $\mathfrak{Q}_i^\Sigma$. Thus $\mathfrak{Q}_i^\Sigma = \mathfrak{Q}_{j(i)}(\Delta)\, T_\Sigma$. Similarly, if $i \geqslant q_0^m(q_0-1)$ then $\mathfrak{Q}_i^\Sigma = \mathfrak{Q}_{q_0-2}(\Delta)\, T_\Sigma$. ∎

If K is ramified over $\mathbb{Q}_p$ then Lemma 2.20 applies, *mutatis mutandis*, to the $\mathfrak{o}\Delta$-lattices $\mathfrak{Q}_j(\Delta)$. In particular, $\mathfrak{Q}_j(\Delta)$ is free over its associated order in $K\Delta$ precisely when $j < (q_0-1)/2$. If $q_0 = 2$, then $\mathfrak{Q}_i^\Sigma = \mathfrak{Q}_0(\Delta)\, T_\Sigma$ for all i, and this lattice is free over its associated order. Thus Theorem 4 fails for $p = 2$. If $q_0 > 2$, it follows from Lemma 5.6 that $\mathfrak{Q}_i^\Sigma$ is free over its associated order precisely when $i < \lfloor q_0/2 \rfloor\, q_0^m$. In particular, if $d \neq q-1$ is a divisor of $q-1$ then $\mathfrak{Q}_{q-1-d}^\Sigma$ is not free over its associated order. Combining these observations with Lemma 2.12, we obtain our final result (from which Theorem 4 follows on taking $q_0 = p$):

THEOREM 6. *Let $q-1 = rd$ with $r > 1$, and, as above, let $\Gamma = \Sigma \times \Delta$ where Σ (respectively, Δ) corresponds to a subspace of $\mathbb{F}_q$ of dimension $m \geqslant 1$ (respectively, of dimension 1) over its subfield $\mathbb{F}_{q_0}$, $q_0 \neq 2$. Let $E = L_d^\Sigma$. Suppose that K is ramified over $\mathbb{Q}_p$. Then $\mathfrak{O}_E$ is not free over its associated order $\mathfrak{A}_{E/K}$. More precisely, let $j(i)$ be defined by* (5.7) *and set $n = \lfloor q_0/2 \rfloor\, q_0^m$. Then*

$$\mathfrak{O}_E \cong \bigoplus_{i \equiv 0 \bmod d} \mathfrak{Q}_{j(i)}(\Delta)\, \varepsilon_i$$

and

$$\mathfrak{A}_{E/K} = \bigoplus_{\substack{0 \leqslant i < n \\ i \equiv 0 \bmod d}} \mathfrak{Q}_{j(i)}(\Delta)\, \varepsilon_i \oplus \bigoplus_{\substack{n \leqslant i \leqslant q-2 \\ i \equiv 0 \bmod d}} \mathfrak{Q}_{q_0-2-j(i)}(\Delta)\, \varepsilon_{q-2-i}.$$

Each summand $\mathfrak{Q}_{j(i)}\varepsilon_i$ of $\mathfrak{O}_E$ with $n \leqslant i \leqslant q-2$ is not free over its associated order $\mathfrak{Q}_{q_0-2-j(i)}(\Delta)\, \varepsilon_{q-2-i}$.

REFERENCES

1. D. Burns, On the equivariant structure of ideals in Galois extensions of fields, preprint King's College London, 1996.
2. N. P. Byott, Toroidal block decompositions for Hopf orders in group algebras, *Proc. London Math. Soc. (3)* **65** (1992), 449–473.

3. N. P. Byott, Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications, *J. Théor. Nombres Bordeaux* **9** (1997), 201–219.
4. N. P. Byott, Associated orders of certain extensions arising from Lubin–Tate formal groups, *J. Théor. Nombres Bordeaux* **9** (1997), 449–462.
5. N. P. Byott and R. J. Chapman, Power sums over finite subspaces of a field, to appear in *Finite Fields and their Applications*.
6. N. P. Byott and G. Lettl, Relative Galois module structure of integers of abelian fields, *J. Théor. Nombres Bordeaux* **8** (1996), 125–141.
7. S.-P. Chan, Galois module structure of non-Kummer extensions, *Arch. Math.* **70** (1998), 286–292.
8. S.-P. Chan and C.-H. Lim, The associated orders of rings of integers in Lubin–Tate division fields over the p-adic number field, *Illinois J. Math.* **39** (1995), 30–38.
9. G. G. Elder and M. L. Madan, Galois module structure of the integers in weakly ramified extensions, *Arch. Math.* **64** (1995), 117–120.
10. B. Erez, The Galois structure of the square root of the inverse different, *Math. Z.* **208** (1991), 239–255.
11. B. Erez and J. Morales, The Hermitian structure of rings of integers in odd degree abelian extensions, *J. Number Theory* **40** (1992), 92–104.
12. A. Fröhlich, Local fields, *in* "Algebraic Number Theory" (J. W. S. Cassels and A. Fröhlich, Eds.), Academic Press, London, 1967.
13. H.-W. Leopoldt, Uber die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. Reine Angew. Math.* **201** (1959), 119–149.
14. G. Lettl, Relative Galois module structure of integers of local abelian fields, *Acta Arith.* **85** (1998), 235–248.
15. R. Miller, "Galois Module Structure in Wild Extensions of the Rational Function Field," Ph.D. thesis, University of Exeter, 1997.
16. P. Ribenboim, "The Book of Prime Number Records," 2nd ed., Springer, New York, 1989.
17. J.-P. Serre, Local class field theory, *in* "Algebraic Number Theory" (J. W. Cassels and A. Fröhlich, Eds.), Academic Press, London, 1967.
18. M. J. Taylor, Formal groups and the Galois module structure of local rings of integers, *J. Reine Angew. Math.* **358** (1985), 97–103.
19. M. J. Taylor, Hopf structure and the Kummer theory of formal groups, *J. Reine Angew. Math.* **375/376** (1987), 1–11.
20. S. Ullom, Integral normal bases in Galois extensions of local fields, *Nagoya Math. J.* **39** (1970), 141–148.
21. L. C. Washington, "Introduction to Cyclotomic Fields," Graduate Texts in Math., Vol. 83, Springer-Verlag, New York, 1982.